Hoeveel ruimte is er voor privacy in het internet van dingen?

Wisman, T.H.A.; Lodder, A.R.

published in
Tijdschrift voor Internetrecht
2010

Hoeveel ruimte is er voor privacy in het internet van dingen?

T.H.A. Wisman en A.R. Lodder[*]

Het internet is niet meer weg te denken uit ons dagelijkse leven. Iedereen heeft het thuis en het gebruik van mobiel internet neemt met de dag toe. Een volgende stap in de ontwikkeling van het internet is om geleidelijk te evolueren van een netwerk van onderling verbonden computers naar een netwerk van onderling verbonden objecten, van boeken tot auto's, van elektrische apparaten tot voedsel, en daarmee een 'internet van dingen' te creëren, aldus de Europese Commissie in 2009.[1] Het Europees Parlement heeft vervolgens in 2010 een resolutie aangenomen waarin zij overweegt dat alle objecten in het dagelijks leven op een gegeven moment voorzien kunnen zijn van RFID-chips, dat het internet van dingen het mogelijk maakt om miljarden apparaten met elkaar te laten communiceren en dat de mogelijkheden in de toekomst alleen maar zullen toenemen. Het Europees Parlement overweegt ook dat het internet van dingen niet tot sociale uitsluiting mag leiden en stelt met klem dat de bescherming van privacy een elementaire waarde vormt. In deze bijdrage richten wij ons op dit laatste aspect, de rol van privacy binnen het internet van dingen.

1.Inleiding

De aanleiding voor het eerste artikel dat ooit over privacy verscheen,[2] lag in de ontwikkeling van het handzame fototoestel en de opkomst van de professionele pers. De combinatie van beide maakte het mogelijk om door te dringen in het domein van het privé en huiselijke leven en hiervan aan het grote publiek verslag te doen. Hierdoor werd wettelijke bescherming van de persoonlijke levenssfeer van belang. Brandeis begreep bovendien dat de technologie nog maar in de kinderschoenen stond en schreef zo'n dertig jaar later in zijn 'dissenting opinion' in de eerste Supreme Court wiretapping case, [3] dat er in de toekomst wellicht manieren zouden worden ontwikkeld die de overheid in staat stellen om geheime informatie weer te geven in de rechtszaal, zonder deze uit geheime lades weg te nemen. De jury kon hierdoor worden blootgesteld aan de meest intieme gebeurtenissen die in en rond het huis plaatsvinden. Tevens vroeg hij zich af of de Amerikaanse Grondwet hier wel bescherming tegen zou bieden. Zo'n 80 jaar later lijkt, ook hier in Europa, deze vraag prangender dan ooit. Technologie is zo ver dat een maatschappij kan worden ingericht waarin de burger wordt verplicht om een groot deel van zijn leven in kaart te (laten) brengen. Dat deze ontwikkeling al in gang is gezet blijkt uit de vergaande maatschappelijke inbedding van internet en de digitalisering van een groot repertoire aan handelingen.

Als het aan de EU ligt wordt het internet uitgebreid met objecten (auto's, schoenen, vervoermiddelen, potjes pindakaas, etc.) die allemaal een IP-adres en/of RFID-tag krijgen waardoor een internet van dingen ontstaat, veelal aangeduid met de Engelse term *The Internet of Things*.[4] De verwachting is dat dit onder meer zal leiden tot een verdergaande versmelting van de digitale en de fysieke wereld.[5] Hoewel dit voor de techno-optimist als een veilig vangnet in de oren kan klinken, ontstaat ook het beeld van een digitale dwangbuis. De EU heeft in haar actieplan voor het internet van dingen[6] aangegeven dat zij, door de grote maatschappelijke veranderingen die deze ontwikkeling ten gevolg zal hebben, hierbij een rol moet spelen. Voor de EU is economische groei veelal leidend, waarbij bescherming van burgerrechten soms onderbelicht kan zijn. Het Europees Parlement heeft deze zomer een resolutie uitgevaardigd[7] waarin overwegingen

* Tijmen Wisman en Arno Lodder zijn beiden verbonden aan de afdeling Transnational Legal Studies van de Vrije Universiteit Amsterdam, alsmede aan het Computer/Law Institute.

1. 'Internet of Things – An action plan for Europe' (Brussel: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of theRegions, 2009) http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf, laatst gezien 1 december 2009.
2. Het bij vrijwel iedereen bekende S. Warren & L.D. Brandeis, 'The Right to Privacy', *Harvard Law Review 5* (1891): 193-220. Nog steeds zeer leesbaar en op internet te vinden op http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
3. Roy Olmstead v. United States of America, 277 U.S. 438, June 4, 1928.
4. Voorzover ons bekend is 2002 een van de eerste keren dat de term Internet van dingen werd gebruikt: C.R. Schoenberger (2002). 'Internet of things', *Forbes Magazine*, March 18 2002. Voor een recent overzicht, zie L. Atzoria, A. Ierab & G. Morabito (2010), 'The Internet of Things: A survey', *Computer Networks: The International Journal of Computer and Telecommunications Networking* Volume 54, Issue 15 (October 2010), p. 2787-2805.
5. Vgl. het concept interrealiteit, J. Van Kokswijk (2003), *Architectuur van een Cybercultuur* (diss. Twente).
6. *EU Internet of Things action plan for Europe* (zie noot 2).
7. 'Resolutie van het Europees Parlement van 15 juni 2010 over het internet van de dingen', zie http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0207+0+DOC+XML+V0//NL, laatst gezien 4 november 2010.

zijn opgenomen die mede bedoeld zijn om ook privacy een plaats te geven binnen het internet van dingen. Hoe dit gerealiseerd kan worden is een lastige vraag.
De huidige staat van de privacy, met stelselmatige verruiming van opsporingsbevoegdheden, uitgebreide registratie van onschuldige burgers en op argwaan berust beleid, levert een somber beeld op. Hoewel er scepsis bestaat over de realiseerbaarheid van het internet van dingen, is dit fenomeen een goede aanleiding om de legitimiteit van de grondslagen en noodzaak van de huidige en toekomstige verwerkingen van persoonsgegevens onder de loep te nemen en een inventarisatie te maken van eventuele gevolgen voor de maatschappij.
In deze bijdrage zullen we eerst het internet van dingen (paragraaf 2) en daarna privacy in het internet van dingen (paragraaf 3) introduceren. De kern bestaat uit een analyse van de betekenis van privacy in het internet van dingen aan de hand van de resolutie van Europees Parlement van afgelopen zomer.

2. Het internet van dingen

Na *ITU Internet Reports 2005: The Internet of Things*, een publicatie van de International Telecommunication Union,[8] is er vanuit de EU sinds vorig jaar nadrukkelijk belangstelling voor dit fenomeen. Het al genoemde *Internet of Things — An action plan for Europe* werd door de EU in 2009 gepubliceerd. Op 1 en 2 juni 2010 werd in Brussel de tweede Annual Internet of Things 2010 conference[9] gehouden, waar ook Neelie Kroes sprak en aangaf voorlopig vooral vragen (o.a. privacy) te hebben die een in te stellen Expert Group moet beantwoorden. Twee weken later, op 15 juni 2010, aanvaardde het Europees Parlement een resolutie over het Internet van Dingen. Hierin is de volgende definitie te vinden:

> het algemeen concept van objecten (zowel elektronische artefacten als voorwerpen voor dagelijks gebruik) die via het internet op afstand kunnen worden gelezen, herkend, aangestuurd, gelokaliseerd en/of gecontroleerd.

'Lezen, herkennen, aansturen, lokaliseren en/of controleren' in het internet van dingen wordt mogelijk door een combinatie van verschillende technologieën. Hieronder volgt een niet-limitatieve lijst van hoe bovenstaande acties kunnen plaatsvinden.
Lezen lijkt af te stammen van de term 'reader' die wordt gebruikt om een apparaat mee aan te duiden waarmee RFID-tags (zoals verwerkt in de OV chip en het 'nieuwe' identiteitsbewijs) zijn 'uit te lezen'. Naast RFID technologie zal IPv6,[10] de opvolger van IPv4, in het internet van dingen een belangrijke rol spelen. Door de komst van IPv6 zijn er genoeg ip-adressen om ieder elektronisch apparaat op de wereld, nu en in de toekomst, uit te rusten met een uniek nummer. Wifi is de technologie waarmee een alom tegenwoordig internet kan worden gecreëerd waarmee IPv6 correspondeert.
Herkenning van dingen is onder andere mogelijk doordat randapparatuur unieke identificatienummers krijgen toegewezen (zoals een MAC-adres), door IP-adressen en unieke RFID-tags.
Aansturen kan plaatsvinden op verschillende manieren, die verderop aan de orde zullen komen.
Lokaliseren is onder andere mogelijk door GSM, GPS, Wifi en RFID.
Controle wordt door de veelheid aan beschikbare informatie steeds eenvoudiger. Controle moet in deze context worden gelezen als beheersen, hoewel het internet van dingen onmiskenbaar het uitvoeren van controle op objecten eenvoudiger maakt. Wat dit betreft is de vertaling in 'gecontroleerd' ongelukkig te noemen, hoewel een Freudiaanse verschrijving ook kan worden verdedigd. Een vergaande beheersing van de publieke ruimte is technisch realiseerbaar, maar de vraag is in hoeverre we bereid zijn met een dergelijk inzet van technologie de ethiek geweld aan te doen. Dit heeft immers tot gevolg dat we een belangrijke menselijke waarde verliezen: het maken van keuzes.[11] Immers als de beheersing zover gaat dat deze het domein van de keuze doorkruist, denk aan auto's die automatisch stoppen voor rode stoplichten, dan verdwijnt de mogelijkheid om onder omstandigheden er voor te kiezen je niet aan de regels te houden.
Het internet van dingen overschrijdt de grenzen van de publieke ruimte en kan in het huis en zelfs het lichaam terecht komen.[12] Momenteel vindt al een digitalisering van de openbare ruimte plaats via onder andere Google Maps en Streetview. Met de toepassing Layar is het mogelijk om de openbare ruimte te scannen en allerhande informatie te verkrijgen over gescande objecten.[13] De op te vragen informatie zal alleen maar toenemen. Door de informatie die op internet beschikbaar is te combineren kan iemand in de toekomst voorbij een huis lopen, zien wie er woont, informatie van een cv op LinkedIn of Monsterboard bekijken, foto's van sociale netwerksites halen, prijs van het huis, in het bezit zijnde auto's, aldaar gevestigde bedrijven, stichtingen, etc. Alle informatie die op internet staat kan nu al eenvoudig gecombineerd worden. Het is alleen de vraag wanneer de komst van een dergelijke ontsluiting van informatie gemeengoed wordt. Naar verwachting zullen mensen daarom kritischer gaan kijken naar de informatie die ze zelf met het publiek delen.

3. Privacy in het internet van dingen

Privacy in het internet van dingen lijkt op het eerste gezicht een paradox. Privacy stamt af van het Latijnse *privare* en betekent zoveel als afzonderen/wegnemen. Privacy is een recht dat moet garanderen dat je zelf kan kiezen met wie of wat je een verbinding aangaat, of sterker nog, of je sowieso wel bereid bent om een verbinding aan te gaan. Het inter-

8. Zie http://www.itu.int/osg/spu/publications/internetofthings/, laatst gezien 11 oktober 2010.
9. Zie http://www.eu-ems.com/about.asp?event_id=55&page_id=345, laatst gezien 11 oktober 2010.
10. Zie ook J.J. Toet, Juridische implicaties bij de invoering van IPv6, *IR* 2010/2, p. 43-47.
11. Zie ook J. Zittrain, *The future of internet*, Yale University Press 2009, p. 122: 'Part of what makes us human are the choices that we make every day about what counts as right and wrong, and whether to give in to temptations that we believe to be wrong. In a completely monitored and controlled environment, those choices vanish.'
12. Zoals het vaak gebruikte voorbeeld van de Rotterdamse Baja Beach club: toegang en afrekenen door een in het lichaam aangebrachte RFID-chip.
13. Zie http://www.layar.com/, laatst gezien 11 oktober 2010.

net van dingen wordt voorgesteld als een verschijnsel waarin allerlei van elkaar losstaande objecten continu met elkaar worden verbonden en op elkaar reageren. Nu is privacy geen absoluut recht, maar wel een recht dat absoluut noodzakelijk is voor een gezonde samenleving. Daarom is het van belang er voor te waken dat het relatieve karakter niet wordt aangegrepen om de huidige uitholling van dit fundamentele recht verder door te zetten. De paradoxale positie die privacy inneemt in een internet van dingen benadrukt het belang van duidelijke voorwaarden voor het gebruik van technologie en sterke rechtsmiddelen om dit recht daadwerkelijk te handhaven, of dit nu op nationaal of internationaal niveau gebeurt.[14]

In het kader van het internet van dingen worden vaak de Europese richtlijnen aangehaald die de bescherming van de informationele privacy beogen.[15] Als het internet van dingen daadwerkelijk de impact gaat hebben die de politiek en het bedrijfsleven ons voorspiegelen, dan is het niet juist om alleen informationele privacy te noemen als waarde die van belang is. De opkomst van dit verschijnsel zal immers ook impact hebben op andere waarden waarop onze samenleving is gefundeerd. Bovendien staat in deze privacy richtlijnen dat ze niet zien op de balans tussen privacy van de burger en de mogelijkheid van lidstaten om maatregelen te nemen in het belang van de openbare veiligheid, defensie, staatsveiligheid, het economisch welzijn van een land en de activiteiten van de Staat op strafrechtelijk gebied. Dit gebied wordt bestreken door art. 8 van het Europees Verdrag van de Mens. Met deze noties in het achterhoofd, is het terecht dat het Europees Parlement opmerkt dat bij de ontwikkeling van het internet van dingen, de bescherming van alle grondrechten belangrijk is.[16] Hierbij denken wij met name aan relationele privacy en het communicatiegeheim.

De afbrokkeling van de privacy is een fenomeen dat grofweg wordt veroorzaakt door een technische en een juridische component. De technische component bestaat uit de opname in de maatschappij van nieuwe technieken en technologieën (slimme camera's, afluistermicrofoons, datamining, koppeling van bestanden en systemen). De juridische component bestaat uit wetgeving die het gebruik van technologie reguleert en die het mogelijk maakt voor justitie en veiligheidsdiensten om op grond van een legitieme basis gebruik te maken van de enorme databases die bedrijven en overheden van burgers bijhouden.[17] De opkomst van een internet van dingen betekent een uitbreiding van deze componenten, omdat door de digitalisering van alledaagse handelingen de hoeveelheid databases met daarin geregistreerde bewegingen van burgers zal toenemen en voor het functioneren van het internet van dingen er zowel in de publieke als private ruimte nieuwe technologieën te vinden zijn. Tevens ligt het in de lijn der verwachtingen dat de ambitie van Europa om de infrastructuur van het internet van dingen te beveiligen en in te zetten om 'maatschappelijke problemen' aan te pakken, zal leiden tot wetgeving die de inzet van het internet van dingen bij de opsporing legitimeert.[18] Tenslotte versterkt de groei van deze twee componenten elkaar onderling en vormen zij een symbiose.

4. Onderwerpen voor nadere reflectie

Het Europees Parlement wijst er in de Resolutie op dat het vaststellen van juridische normen waarmee de eerbiediging van de fundamentele waarden en de bescherming van persoonsgegevens en privacy wordt versterkt, een voorwaarde is voor de bevordering van de technologie. Enerzijds geeft het Parlement aan dat het internet van dingen en de daaraan gekoppelde toepassingen de komende jaren van grote invloed zal zijn op het dagelijkse leven van de Europeanen, hun gewoonten en tot tal van economische en sociale veranderingen zal leiden. Anderzijds moet de consument kunnen kiezen of hij al dan niet aan het internet van dingen deelneemt en onder meer de mogelijkheid krijgt om specifieke 'Internet van dingen' -technologieën af te wijzen, zonder dat andere toepassingen of apparaten in het geheel worden gedeactiveerd. Waakzaamheid is hier geboden, want zeker is dat hoe meer massa het internet van dingen krijgt, hoe meer waarde het zal hebben en hoe belangrijker het dus zal zijn voor de economie. Op deze manier belandt de EU in een spagaat. Kijkend naar de huidige bescherming van privacy op internet en wetende dat een belangrijk doel van de EU het bevorderen van de interne markt is, resteert de vraag wat een vergaande ontwikkeling van het internet van dingen betekent voor de privacy van de burger?

Hieronder zullen relevante onderdelen van de Resolutie worden aangehaald en van commentaar voorzien. Daarmee ontstaat een goed beeld van de punten die nadere aandacht vereisen bij de ontwikkeling van het internet van dingen en de daarop toepasselijke normen inzake de bescherming van de persoonlijke levenssfeer.

5. Welke verwachtingen?

> 'B. overwegende dat het internet van de dingen aan de verwachtingen van de samenleving en de burgers kan voldoen, maar dat onderzoek nodig is om erachter te komen welke verwachtingen dat zijn en op welke punten gevoeligheden of bezorgdheden met betrekking tot de persoonlijke levenssfeer eventueel bepaalde toepassingen in de weg staan,'

Kennelijk doet het ertoe in hoeverre toepassingen in het internet van dingen als een inbreuk op de persoonlijke levenssfeer worden ervaren door de mensen die worden betrokken in het onderzoek. De mening van de burger als graadmeter gebruiken voor een inbreuk op de persoonlijke levenssfeer bergt het gevaar in zich dat minder evidente inbreuken over het hoofd worden gezien door een panel, hetgeen niet gelijk staat met het verschaffen van een legitieme basis voor een verwerking. Er lijkt in deze overweging geen rekening te worden gehouden met het feit dat toepassingen zo kunnen worden gebouwd dat ze geen inbreuk maken op de bescherming van de persoonlijke levenssfeer. Sterker nog, de gevoeligheden en bezorgdheden rond de persoonlijke levenssfeer worden in de laatste zin in de hoek gezet van hin-

14. Zie http:/www.cbpweb.nl/Pages/med_20100921_gpen.aspx, laatst gezien op 23 september, 2010.
15. Richtlijn 95/46/EG en 2002/58/EG.
16. 'Resolutie van het Europees Parlement van 15 juni 2010 over het internet van de dingen', 56. is ervan overtuigd dat alle grondrechten, niet alleen met betrekking tot privacy, in het kader van de ontwikkeling van het internet van de dingen moeten worden beschermd.
17. A.H. Vedder en mr. J.G.L. van der Wees, 'Hoe veilig is de privacy van de doorsnee burger sinds 9/11?', *Privacy&Informatie* 10 (2007): 4.
18. Zie http://www.indect-project.eu/, laatst gezien 11 oktober 2010.

dernissen, in plaats van bedenkingen die serieus dienen te worden genomen en die eventueel kunnen worden voorkomen door de manier waarop een systeem wordt vormgegeven.

6. Feitelijke macht

> 'E. overwegende dat onder 'internet van de dingen' wordt verstaan het algemeen concept van objecten (zowel elektronische artefacten als voorwerpen voor dagelijks gebruik) die via het internet op afstand kunnen worden gelezen, herkend, aangestuurd, gelokaliseerd en/of gecontroleerd, F. gezien de in de komende jaren te verwachten snelle ontwikkelingen op het gebied van het internet van de dingen en de noodzaak van een veilig, transparant en multilateraal beheerssysteem daarvoor,'

In *The future of internet* van Zittrain wordt gesproken over een rechtszaak tussen twee bedrijven, TiVo en EchoStar, waarin de laatste door de rechter werd veroordeeld om de digitale opname-functie in één van hun producten uit te schakelen.[19] Dit gold echter niet alleen voor de producten die ze nog gingen verkopen, maar ook voor de producten die al waren verkocht. De schotelsystemen van EchoStar 'bellen' periodiek naar EchoStar en vragen om geactualiseerde programma's voor de interne software. Op deze manier kan de functionaliteit van een apparaat dus van buitenaf worden gewijzigd, of in het ergste geval permanent worden verwijderd. Dit probleem is niet nieuw, door middel van vage updates waarvan de meeste mensen niet weten wat ze precies doen, zijn zij allang geen baas meer op hun eigen computer. Dit benadrukt eens te meer hoe moeilijk het is om een beheerssysteem daadwerkelijk veilig, transparant en multilateraal te maken. Gezien de verhoudingen tussen bedrijven en consumenten/overheid en burgers lijkt een top-down-constructie onvermijdelijk, waarbij de eigenaren van dit beheerssysteem, de overheid/het bedrijfsleven/of een combinatie van beide , vergaande bevoegdheden en mogelijkheden krijgen om feitelijke macht uit te oefenen over de voorwerpen die zijn opgenomen in dit internet van dingen. Op deze manier kunnen ze diep ingrijpen in de autonomie van het individu. Een dergelijke bevoegdheid moet, naast kenbaar zijn, voldoen aan wettelijke waarborgen die geen ruimte laten voor willekeur. Het is met name in geval van het daadwerkelijk aansturen van objecten op afstand door overheid en bedrijfsleven van belang dat dit kenbaar wordt gemaakt aan voor het gevolgde object relevante entiteit(en).

> '26. verzoekt de Commissie te overwegen ivd (internet van dingen) -toepassingen te gebruiken ter bevordering van een aantal bestaande EU-initiatieven zoals 'ICT voor energie-efficiëntie', 'slimme meters', 'energie-etikettering', 'energieprestaties van gebouwen' en 'bescherming tegen namaakgeneesmiddelen en andere namaakproducten;'

Dit is een interessant verzoek, omdat de slimme meter erbij wordt betrokken. Dit is een meter die het stroomgebruik ieder kwartier uitleest en online verzendt naar de netbeheerder. Minister van der Hoeven probeerde deze meter nog te verplichten op straffe van een geldboete of gevangenisstraf, maar hier heeft de Eerste Kamer tegen gestemd. Ondertussen worden deze meters nog steeds in nieuwbouwhuizen geplaatst en heeft de burger niet de keuze om het zenden van de signalen uit te schakelen waardoor de burger toch min of meer zit opgescheept met een spionage-kastje.[20]
De slimme meter is tevens een goed voorbeeld van het op een afstand controleren of aansturen van iets, daar deze het onder andere mogelijk maakt om van een afstand het stroomgebruik van een huishouden bij te houden en/of af te sluiten. Naast kijken naar de wettelijke voorwaarden waaronder dit zou mogen, kunnen we de vraag stellen of een dermate vergaande verschuiving van de feitelijke macht naar de sterkere partij (de energieleverancier) op zichzelf wel wenselijk is. Een tijd terug was er op het programma Radar een aflevering gewijd aan onbetrouwbare gasmeters, waarvan bij enkele exemplaren de meters zelfs nog liepen, terwijl ze waren afgesloten van het gasnet. Het is goed voor te stellen dat hieruit een geschil voortvloeit tussen de afnemer en de leverancier en het lijkt ons hoogst onwenselijk als de laatste in dat geval de feitelijke macht in handen heeft en door middel van dreiging met afsluiting betaling kan afdwingen. Het is geenszins duidelijk wat de noodzaak van een dergelijke gedetailleerde registratie van stroomgebruik zou zijn. Het is nauwelijks voorstelbaar dat het belang dat producenten hebben bij het anticiperen op pieken en dalen in stroomgebruik, niet zou kunnen worden bereikt met minder ver ingrijpende maatregelen, zoals registratie op wijkniveau. Als je de burger echt vrij wilt laten bewegen in een internet van dingen, dan moet het zijn keuze zijn of hij dergelijke gedetailleerde informatie wil delen.

7. RFID en een recht op stilte

> '16. benadrukt dat de consument het recht op privacy heeft via een opt-in- en/of een 'privacy op maat'-systeem waarbij de tags op het verkooppunt automatisch worden gedeactiveerd tenzij de consument uitdrukkelijk anders beslist; wijst in dit verband op het advies van de Europese Toezichthouder voor gegevensbescherming; wijst erop dat in een zo vroeg mogelijk stadium van de ontwikkeling en uitrol van ivd-technologieën aandacht moet worden geschonken aan privacy en veiligheid; wijst erop dat RFID-toepassingen moeten worden ingezet in overeenstemming met de privacy- en gegevensbeschermingsregels zoals neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie; verzoekt de Commissie zich te bezinnen op het recht van de burger om voor ivd-vrije producten te kiezen en het recht om op elk gewenst moment de verbinding met de netwerkomgeving te verbreken;
> 19. verzoekt de fabrikanten het 'recht op stilzwijgen' van de chips te garanderen door ervoor te zorgen dat RFID-tags verwijderbaar zijn of door de consument na de aanschaf gemakkelijk kunnen worden gedeactiveerd;'

Het recht op stilzwijgen lijkt erg op 'het recht op stilte', een term die we tegenkomen in het actieplan van de EU en het idee uitdrukt dat mensen zich altijd moeten kunnen afslui-

19. Zittrain 2009 (zie noot 12), p. 103.
20. Zie http://www.wijvertrouwenslimmemetersniet.nl/, laatst gezien 11 oktober 2010.

ten van de genetwerkte omgeving.[21] Een dergelijk recht impliceert de onmogelijkheid van verplichte deelname aan ivd-technologieën,[22] alhoewel met de huidige gang van zaken rond de ov-chipkaart en het paspoort moeilijk te zeggen is of een dergelijk recht van enige waarde is buiten de grenzen van het huis. Een slimme meter die alleen maar persoonsgebonden met een bepaalde tijdsinterval het gebruik van stroom/water/gas registreert in nieuwbouwhuizen standaard inbouwen beschouwen wij daarom ook als een handeling die rechtstreeks tegen een dergelijk recht zou ingaan.
Het recht op stilzwijgen lijkt echter minder ver te gaan en alleen te zien op RFID-tags. Consumenten moeten volgens het EP de optie krijgen om de chip op gekochte producten in dan wel uit te schakelen. Hoe ver het recht op stilzwijgen gaat is maar zeer de vraag. In het rapport van ITU over het internet van dingen wordt al gesproken over een RFID systeem in een auto dat door de wet wordt verplicht. In de huidige drang om een risicoloze samenleving te creëren is het goed voorstelbaar dat RFID systemen worden verplicht in auto's om bepaalde wettelijke normen te handhaven die bijdragen aan de veiligheid. Het rijbewijs dat inmiddels voorzien is van een chip is in de toekomst de ideale persoonsgebonden opstartsleutel, die vereist kan zijn om je auto op te starten. Ook hier speelt feitelijke macht weer een grote rol, want de overheid zou in de toekomst via een database en controlecentrum kunnen bepalen wiens rijbewijs geactiveerd blijft. In een geschil met de overheid zou deze kunnen beslissen om jouw rijbewijs te deactiveren. Dit is wederom een voorbeeld van een zaak die op een afstand wordt gecontroleerd door een dominante partij. Perfecte handhaving komt daarmee in zicht, maar hoe wenselijk is het om een omgeving te creëren die perfect handhaaft en waar je aan de regels houden niet langer een keuze is, maar een van bovenaf geforceerde situatie? Externe dwang die het individu aanzet tot een keuze, heeft een negatieve invloed op de betrokkenheid die bij het uitvoeren van een handeling wordt ervaren door het individu. Foucault zei reeds dat er geen ethiek kan zijn zonder keuzes, maar je zou hem kunnen tegenwerpen dat er in dit specifieke voorbeeld geen ruimte voor ethiek in het verkeer is. Dergelijke scheve machtsverhoudingen kunnen misbruik bij de uitvoerende macht in de hand werken, daarom is het aan de wetgevende en de rechterlijke macht om te zorgen dat er een balans wordt gevonden.
Tevens klinkt het verzoek aan het adres van de fabrikanten om een 'recht op stilzwijgen' te garanderen (zie 19) als een zwaktebod. Als bedrijfsmodellen, waarbij de chips ingeschakeld blijven of waarbij het uitschakelen ernstige nadelen met zich meebrengt, beloven bij te dragen aan een grotere winst, dan is het zeer onwaarschijnlijk dat een bedrijf zich iets van dit verzoek zal aantrekken. Nu zie je al bij het besturingssysteem van een Android telefoontoestel van Google dat deze standaard laat weten waar de gebruiker zich bevindt. De concurrent Apple claimt in de privacyvoorwaarden het recht om locatiegegevens te verzamelen, beheren, verwerken, delen en verkopen aan partners en licentiehouders. Dat je de keuze hebt geen Apple aan te schaffen is natuurlijk waar, maar wat nou als iedere aanbieder van mobiele telefoons dezelfde truc toepast? Is hier geen taak voor de wetgever om tegen dergelijke onredelijke voorwaarden op te treden, of is het aan de burger om zijn telefoon thuis te laten?
Het zou een stuk sterker overkomen als het Europees Parlement zou vaststellen dat uit de Richtlijn 95/46/EG een verplichting voor de fabrikant voortvloeit om bij het ontwerp van zijn producten het recht op stilte voor de consument in acht te nemen. Om een dergelijke verplichting af te dwingen, zou er een marktautoriteit moeten worden aangewezen die fabrikanten die niet voldoen aan de wet, substantiële boetes kan opleggen.

8. Privacy als elementaire waarde?

> '4. stelt met klem dat de bescherming van de privacy een elementaire waarde vormt en dat alle gebruikers zeggenschap over hun persoonsgegevens moeten hebben; dringt er daarom op aan dat de richtlijn inzake gegevensbescherming afgestemd wordt op de huidige digitale omgeving;
> 6. wijst er met nadruk op dat het vaststellen van juridische normen waarmee de eerbiediging van de fundamentele waarden en de bescherming van persoonsgegevens en privacy wordt versterkt, een voorwaarde is voor de bevordering van de technologie;'

De Europese Commissie besloot onlangs nog om de herziening van de privacyrichtlijn met een jaar uit te stellen.[23] Zeker met de toenemende mogelijkheden is het van groot belang dat gebruikers zeggenschap houden over hun gegevens. In een digitale omgeving waarbij verwerkingen steeds vaker voorkomen, zal het lang niet altijd duidelijk zijn wie nou welke gegevens verwerkt. Om interactie in een dergelijke omgeving soepel te laten verlopen is continu toestemming vragen voor een verwerking geen optie. Zeggenschap, toestemming, het informeren van de betrokkene en nog vele andere verplichtingen die uit de huidige Richtlijn voortvloeien zullen in een digitale omgeving moeten worden geïmplementeerd. Voordat er wordt gekeken naar deze rechten, dient men echter eerst de vraag te stellen of een verwerking van persoonsgegevens op zichzelf wel noodzakelijk is.
Een goede illustratie van het onjuist hanteren van de Richtlijn 95/46/EG toonde het CBP toen het oordeelde dat de gepersonaliseerde ov-chipkaart van de NS toelaatbaar was. In een artikel op Webwereld geeft een medewerker van het CBP zelfs te kennen dat er oplossingen zijn waarbij minder persoonsgegevens zouden moeten worden verwerkt en waarbij de inbreuk op de persoonlijke levenssfeer minder ver gaat, maar dat hetgeen de NS bij hen heeft voorgelegd desalniettemin voldoet aan de wet.[24] De wet stelt echter dat er moet worden voldaan aan het vereiste van noodzakelijkheid en nu het CBP zelf aangeeft dat de verwerking op

21. *EU Internet of Things action plan for Europe* (zie noot 2).
22. Friedewald, M., R. Lindner & D. Wright (eds.), *Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence*, SWAMI Deliverable D3: A report of the SWAMI consortium to the European Commission under contract 006507, June 2006. http://swami.jrc.es, p. 74. In door de EU gefinancierde SWAMI-onderzoek wordt nog geen halve pagina besteedt hieraan. Kenmerkend en tevens zorgelijk is dat personen die behoefte zouden hebben aan een recht op stilte worden weggezet als wezensvreemde individuen die niet mee kunnen komen met technische vooruitgang.
23. Zie http://www.solv.nl/weblog/uitstel-herziening-privacy-richtlijn/17174, laatst gezien 11 oktober 2010.
24. Zie http://webwereld.nl/nieuws/53469/cbp-sluit-privacy-deal-met-ns-over-ov-chipkaart.html, laatst gezien op 27 september 2010.

de persoonlijke OV-chipkaart ook minder verstrekkend had kunnen zijn, kan nooit aan dit vereiste zijn voldaan. Het lijkt er veeleer op dat onevenwichtige machtsverhoudingen ertoe leiden dat dergelijke evidente inbreuken op de huidige wet door de vingers worden gezien, dan wel uit onmacht worden gedoogd. Het bedrijfsleven lukt het zo om de consument in te kapselen in een digitale omgeving en de mogelijkheden nemen alleen maar toe. Er zijn nu al reclameborden met ingebouwde camera's die reageren op het geslacht, het humeur en de kijkrichting van de voorbijganger. Wanneer zulke reclameborden meer winst zullen genereren zal het bedrijfsleven dergelijke vormen van marketing verdedigen door te stellen dat hier geen sprake is van een verwerking van persoonsgegevens. Zoals sociale netwerksites menen geen persoonsgegevens te verwerken als ze alleen kijken waar je op klikt, maar daaraan niet je naam kunnen koppelen. Een maatschappij gestoeld op een dergelijke primitieve benadering van het concept privacy zou in optima forma al het handelen van mensen kunnen registreren zolang er niet de naam van Jan of Piet aan wordt verbonden.[25] Een dergelijke interpretatie getuigt van weinig visie.

9. Slot

Wat de EU precies ambieert met het Internet van dingen is vooralsnog onduidelijk. Door echter niet duidelijke grenzen te stellen, wordt zonder noodzakelijke waarborgen de deur geopend voor bedrijven in deze lonkende industrie die actief door de EU en Den Haag wordt gestimuleerd.[26]

Vertrouwen in een internet van dingen kan er alleen zijn als deelname hieraan berust op een vrijwillige basis en de partijen die er aan werken transparant zijn over de bedoelingen en werkwijzen.

Om alle betrokken partijen, overheid/bedrijfsleven/burgers, op één lijn te krijgen is het noodzakelijk dat er voor alle partijen voordeel is te behalen. Er moet worden gewerkt aan een duidelijk juridisch kader waarin het internet van dingen zich kan ontwikkelen op een legitieme basis. Met in het achterhoofd de wijze waarop de OV-chipkaart is geïntroduceerd kan worden geconcludeerd dat duidelijker moet worden wanneer een verwerking van persoonsgegevens is toegestaan. Daarnaast moeten er duidelijke voorwaarden worden gesteld voor inzet van technologie die registratie van personen of persoonsgebonden objecten mogelijk maakt en daarmee een inbreuk kan vormen op iemand zijn privacy. Deze voorwaarden kunnen uiteindelijk resulteren in een recht op stilte, maar het is zeer de vraag hoe ver de bescherming van een dergelijk recht gaat.

Naast een duidelijker juridisch kader is er behoefte aan een toezichthouder die daadwerkelijke macht kan uitoefenen. Een CBP die in haar handhavende bevoegdheden maximaal kan dreigen met een last onder dwangsom, is als een waakhond zonder tanden, die wordt dus niet serieus genomen.[27]

Tenslotte is er een groot risico dat het internet van dingen een verschuiving van de feitelijke macht inhoudt, waardoor grote maatschappelijke entiteiten controle verkrijgen ten koste van de autonomie van het individu. Het maken van keuzes, die niet tot stand komen door externe dwang, is in een ongebreidelde vorm van het internet van dingen moeilijk te realiseren.

Voordat er kan worden gesproken over mogelijkheden en kansen, moeten de EU, het Europees Parlement, nationale regeringen en alle betrokken bedrijven, erkennen dat privacy en de bescherming van de persoonlijke levenssfeer niet een hindernis is, maar een noodzakelijke voorwaarde voor een vrije samenleving waarin de basis voor interactie vertrouwen is. Met iedere nieuwe gedwongen registratie, wordt er in feite tegen de burger gezegd dat de maatschappij hem of haar niet vertrouwt. Nu de registratie van handelingen steeds meer gaat omvatten, beginnen zelfs de struisvogels onder ons die eerst nog meenden 'niks te hebben verbergen',[28] in te zien dat deze naïeve gedachte eerder was ingegeven door kortzichtigheid dan door inzicht. Hoe willen we in de maatschappij staan? Zijn gehoorzaamheid, risicobeperking en controle de waarden waarop wij onze samenleving willen baseren? Of moet de massa soms ook buigen voor de rechten van het individu?

In het boek 'The Fountainhead' van Ayn Randt, staat de excentrieke architect Howard Roark terecht in een zaak waarin het belang van de massa en het individu recht tegenover elkaar staan. Wij sluiten dit artikel af met een quote uit zijn verdediging: 'Civilisation is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilisation is the process of setting man free from men.'

25. Zie hierover uitgebreider T. Wisman en M. van der Linden-Smith, 'My secret life as an average person. Anonieme gegevensverzamelingen en informationele privacy', *IR* 2008/4, p. 86-89.
26. Zie http://www.syntens.nl/ndiv-nieuw/Pages/home.aspx, laatst gezien 11 oktober 2010.
27. Zie in deze zin ook J.J. Borking (2010), *Privacy als code* (diss. Leiden).
28. Daniel J. Solove, "I've Got Nothing to Hide' and Other Misunderstandings of Privacy', *San Diego Law Review*, Vol. 44, p. 745, 2007, online beschikbaar op http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565&rec=1&srcabs=174508.